REMARKS

Favorable reconsideration of this application, in light of the following discussion, is respectfully requested.

Claims 1-15 are currently pending. No claims have been amended herewith.

In the outstanding Office Action, Claims 1-4 were rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent Application Publication No. 2004/0088542 to Daude et al. (hereinafter "the '542 application") in view of U.S. Patent Application Publication No. 2004/0266420 to Malinen et al. (hereinafter "the '420 application"); Claims 5, 7, and 8 were rejected under 35 U.S.C. § 103(a) as being unpatentable over the '542 and '420 applications, further in view of U.S. Patent Application Publication No. 2003/0039240 to Sutanto (hereinafter "the '240 application"); Claim 6 was rejected under 35 U.S.C. § 103(a) as being unpatentable over the '542, '420, and '240 applications, further in view of U.S. Patent Application Publication No. 2004/0208151 to Haverinen et al. (hereinafter "the '151 application"); and Claims 9-15 were rejected under 35 U.S.C. § 103(a) as being unpatentable over the '542 application in view of the '240 application.

Applicants wish to thank the Examiner for the interview granted Applicants' representative on April 10, 2009, at which time the outstanding rejection of the claims was discussed. In particular, the functions of the mediating apparatus recited in Claims 1 and 9 were discussed. Specifically, Applicants representative presented arguments that the communication means recited in Claim 9 is not disclosed by the '542 application. At the conclusion of the interview, the Examiner agreed to reconsider the rejection of Claims 1 and 9 when a response is filed.

Claim 1 is directed to a remote-access VPN mediating method in a system wherein VPN client units and a VPN gateway unit are connected to an IP network; communication units are connected to a local area network placed under the management of the VPN

9

gateway unit; and a remote-access VPN by a tunneling protocol is implemented between an

arbitrary one of the VPN client units and the VPN gateway unit connected to said IP network

and an arbitrary one of the communication units connected to the local area network placed

under the management of the VPN gateway unit, where VPN represents virtual private

network, the method comprising the steps of: (a) sending an access control list containing

information indicative of a private IP address assigned to said communication unit to a

mediating apparatus on said IP network from said VPN gateway unit; (b) storing said access

control list in said mediating apparatus in correspondence to said VPN gateway unit; (c)

retrieving, by said mediating apparatus, an IP address of said VPN gateway unit in response

to a request from said VPN client unit, acquiring the private IP address of the corresponding

communication unit from said access control list, sending the acquired IP address of said

VPN gateway unit and the acquired private IP address to said VPN client unit, sending an IP

address of said VPN client unit to said VPN gateway unit, generating mutual authentication

information for setting up an authenticated encrypted tunnel between said VPN client unit

and said VPN gateway unit, and sending said mutual authentication information to both of

said VPN client unit and said VPN gateway unit; and (d) setting up said authenticated

encrypted tunnel between said VPN client unit and said VPN gateway unit by use of said

mutual authentication information, and implementing remote access through said encrypted

tunnel by use of the private IP address of said communication unit.

Regarding the rejection of Claim 1 under 35 U.S.C. § 103(a), the Office Action

asserts that the '542 application discloses everything in Claim 1 with the exception of setting

up an authenticated encrypted tunnel between the VPN client unit and the VPN gateway

unit,[1] and relies on the '420 application to remedy that deficiency.

---

[1] See page 6 of the Office Action.

The '542 application is directed to a method for permitting a first device on a virtual

private network to communicate with a second device outside the virtual private network,

including the steps of authenticating, at an interconnection device, the first device;

authenticating, at the interconnection device, VPN parameters related to connecting and

forwarding characteristics of the VPN with which the first device is associated; and

forwarding data from the first device to the second device via the VPN and the

interconnection device. In particular, the '542 application discloses that routing tables for

setting a connection between VPNA-VPNC on the network 170 and VPND-VPNF on the

network 180 are held in virtual routers VR1-VR5, and that each of F&FE 261 to 266

performs routing for an input packet by referring to the corresponding ones of the VRs.[2]

Further, the '542 application discloses that the interconnection between devices 100, 110, 120

and 130, 140, and 150 on different VPNs are made through gateway 160, which provides

information necessary for interconnection upon request.

However, Applicants respectfully submit that the '542 application fails to disclose

sending an access control list containing information indicative of a private IP address

assigned to the communication unit **to a mediating apparatus** on the IP network from the

VPN gateway unit, as recited in Claim 1. Rather, the background section of the '542

application clearly states that the access control list resides in the routers. See paragraphs

[0044]-[0046] in the '542 application. Applicants respectfully submit that the routers

disclosed by the '542 application do not correspond to the mediating apparatus recited in

Claim 1.

Further, Applicants respectfully submit that the '542 application fails to disclose

storing the access control list in the mediating apparatus in correspondence to the VPN

gateway unit, as recited in Claim 1. Rather, paragraph [0044] in the '542 application merely

---

[2] See Fig. 2 and para. [0101] in the '542 application.

11

discloses that the access control list reside in routers that control the traffic flow, but does not describe anything about storing an ACL in correspondence with a VPN gateway unit, since each router holds only its own ACL.

Further, Applicants respectfully submit that the '542 application fails to disclose retrieving, by the mediating apparatus, an IP address of the VPN gateway unit in response to a request from the VPN client unit, acquiring a private address of the corresponding communication unit from the access control list, sending the acquired IP address of the VPN gateway unit and the acquired private IP address to the VPN client unit, sending an IP address of the VPN client unit to the VPN gateway unit, generating mutual authentication information for setting up an authenticated encrypted tunnel between the VPN client unit and the VPN gateway unit, and sending the said mutual authentication information to both of the VPN client unit and the VPN gateway unit, as recited in amended Claim 1.

Rather, the '542 application merely discloses that the interconnecting device (gateway 160) identifies VPN parameters relating to connecting and forwarding characteristics of the VPN, but paragraph [0044] of the '542 application describes that the conventional ACL-based management system basically manages ACLs residing in routers, but does not disclose anything about the mediating apparatus that retrieves a private address of the communication unit from the ACL held in the mediating apparatus and sending it to the VPN client unit, as recited in Claim 1. Further, Applicants note that paragraph [0095] of the '542 application discloses that the F&FE of the gateway 160 identifies a destination IP address from the IP source address in a receipt packet, but does not disclose anything about the mediating apparatus that sends an IP address of the VPN client to the VPN gateway unit through which the VPN client unit is trying to access a communication unit, as required by Claim 1. Further, Applicants note that paragraph [0108] of the '542 application discloses that routing configuration filtering rules are formulated in the digital certificate. However, Applicants

12

respectfully submit that this disclosure is unrelated to mutual authentication in which each of the two parties confirm authenticity of the counter-party. Moreover, the routing rules are provided in virtual routers VR1-VR5 in the gateway 160 in the '542 system, and the F&FEs 261-266 perform connection with reference to the routing rules downloaded from the VR1-VR5 routers.

Further, Applicants note that, during the interview, the Examiner indicated that the '542 gateway 160 was meant to read on the claimed mediating apparatus, and that the claimed gateway unit is part of one of the VPNs D, E, or F, shown in '542 Figure 2, but is not specifically identified in the Office Action. However, Applicants submit that the '542 application does not disclose the step of sending the acquired IP address of the VPN gateway unit and the acquired private IP address to the VPN client unit, as required by Claim 1.

Further, Applicants note that the steps in Claim 1 are clearly part of a process for "setting up said authenticated encrypted tunnel between said VPN client unit and said VPN gateway unit…," such that the extracting of source and destination IP addresses in a packet by a router/gateway unit, as disclosed by the '542 application, is (1) irrelevant to the process of Claim 1, and (2) is not a disclosure of sending the two claimed IP addresses to the VPN client, as required by Claim 1.

The '420 application is directed to a system for providing secure mobile connectivity that implements mobile IP home agent functionality via distributed components. In particular, the '420 application is directed to a system for a secure connection between mobile nodes and an internal private network using VPN technology. Paragraph [0004] of the '420 application discloses that a VPN gateway sets a tunnel secured by authentication and encryption.

However, Applicants respectfully submit that the '420 application fails to cure the deficiencies of the '542 application with respect to steps a, b, and c recited in Claim 1. In

particular, the '420 application fails to disclose the <u>mediating apparatus</u> recited in Claim 1.

Specifically, the '420 application fails to disclose the step of sending an access control list

containing information indicative of a private IP address assigned to the communication unit

<u>to a mediating apparatus</u> on the IP network from the VPN gateway unit or storing the access

control list in the mediating apparatus in correspondence to the VPN gateway unit. Further,

the '420 application fails to disclose retrieving, <u>by the mediating apparatus</u>, an IP address of

the VPN gateway unit in response to a request from the VPN client unit, acquiring the private

IP address of the corresponding communication unit from the access control list, **sending the**

acquired private IP address of the VPN gateway unit and the acquired private address

to the VPN client unit, and sending an IP address of the VPN client unit to the VPN gateway

unit, as required by Claim 1.

Thus, no matter how the teachings of the '542 and '420 applications are combined,

the combination does not teach or suggest the <u>mediating apparatus</u> and <u>steps (a), (b) and (c)</u>

recited in Claim 1. Accordingly, Applicants respectfully traverse the rejection of Claim 1

under 35 U.S.C. § 103(a) as being unpatentable over the '542 and '420 applications.

Claim 9 is directed to a remote-access VPN **mediating apparatus** which is built on

an IP network to implement a remote-access VPN representing virtual private network in a

system wherein: VPN client units and a VPN gateway unit are connected to the IP network;

communication units are connected to a local area network placed under the management of

the VPN gateway unit; and a remote-access VPN by a tunneling protocol is implemented

between an arbitrary one of said VPN client units and said VPN gateway unit connected to

said IP network and an arbitrary one of said communication units connected to said local area

network placed under the management of said VPN gateway unit, said apparatus comprising:

(1) ACL storage means for storing an access control list, hereinafter referred to as ACL, sent

from said VPN gateway unit and containing information indicative of a private IP address

assigned to said communication unit; (2) authentication/access authorization control means

for authenticating said VPN client unit and said VPN gateway unit, and for executing access

authorization control; (3) IP address acquiring means for referring to said access control list

to acquire the private IP address assigned to said communication unit, and for searching a

domain name server to acquire an IP address assigned to said VPN gateway unit; (4)

authentication information generating means for generating mutual authentication

information for setting up an authenticated encrypted tunnel between said VPN client unit

and said VPN gateway unit; and (5) communication means for sending the IP address of said

VPN gateway unit, the private IP address of said communication unit and said mutual

authentication information to said VPN client unit, and for sending the IP address of said

VPN client unit and said mutual authentication information to said VPN gateway unit.

Regarding the rejection of Claim 9 under 35 U.S.C. § 103(a) the Office Action asserts

that the '542 application discloses everything in Claim 9 with the exception of IP address

acquiring means for referring the access control list to acquire the private IP address assigned

to the communication unit, and for searching a domain name server to acquire the IP address

assigned to the VPN gateway unit, and relies on the '240 application to remedy that

deficiency.

As discussed above, the '542 application is directed to a method for permitting a first

device on a VPN to communicate with a second device outside the VPN. However, as

discussed above, the '542 application fails to disclose a mediating apparatus. In particular,

the '542 application fails to disclose ACL storage means for storing an access control list sent

from the VPN gateway unit, as well as authentication/authorization control means for

authenticating the VPN client unit and the VPN gateway unit. Further, the '542 application

fails to disclose functionality of the IP address acquiring means, the authentication

information generating means, and the communication means recited in Claim 9. As

15

discussed above with respect to Claim 1, the '542 application does not disclose sending the two claimed IP addresses to the VPN client unit as recited in Claim 9.

The '240 application is directed to a method of accessing an embedded web server of a broadband access terminal. In particular, in paragraph [0031], the '240 application discloses that the user terminal sends an HTTP request to the website of the obtained IP address to the gateway. However, Applicants respectfully submit that the '240 application fails to cure the deficiencies of the '542 application with respect to the mediating apparatus recited in Claim 9. Further, Applicants note that the Office Action does not rely on the '240 application as disclosing these limitations. In particular, Applicants respectfully submit that the '240 application fails to disclose the ACL storage means, IP address acquiring means, the authentication information generating means, and the communication means of a mediating apparatus, as recited in Claim 9.

Thus, no matter how the teachings of the '542 and '240 applications are combined, the combination does not teach or suggest the ACL storage means, the IP address acquiring means, the authentication information generating means, and the communication means recited in Claim 9. Accordingly, Applicants respectfully traverse the rejection of Claim 9 (and all associated dependent claims) under 35 U.S.C. § 103(a).
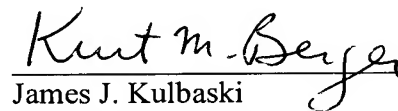
Regarding the rejection of dependent Claims 5-8 under 35 U.S.C. § 103(a) Applicants respectfully submit that the '240 and '151 applications fail to remedy the deficiencies of the '542 and '420 applications, as discussed above. Regarding dependent Claim 5, the '240 application relates to a method for accessing a webserver and discloses MAC addresses, but does not disclose searching a domain name server to acquire the IP address assigned to the VPN gateway unit. Accordingly, Applicants respectfully traverse the rejections of Claims 5-8 under 35 U.S.C. § 103.

16

Thus, it is respectfully submitted that independent Claims 1 and 9 (and all associated

dependent claims) patentably define over any proper combination of the cited references.

Consequently, in light of the above discussion, the outstanding grounds for rejection

are believed to have been overcome. The present application is believed to be in condition

for formal allowance. An early and favorable action to that effect is respectfully requested.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Customer Number

22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 08/07)

Kurt M. Berger

James J. Kulbaski
Attorney of Record
Registration No. 34,648

Kurt M. Berger, Ph.D.
Registration No. 51,461

I:\ATTY\KMB\267'S\267285US\267285US-AM2-MODIFIED.DOC

17